

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
6870 West Kathleen Court, Apartment 7,
Franklin, Wisconsin 53132

Case No.23-1832M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 11/6/2023 *(not to exceed 14 days)*
xx ☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued:10/23/2023 @ 10:54 a.m.

ing, the later specific date of _____



Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to Be Searched

The residence of Jahnell Easley, 6870 West Kathleen Court, Apartment 7, Franklin, Wisconsin, 53132. Apartment 7 is on the first floor of the north entrance to a two story apartment building. The exterior of the first floor of the apartment building has brown bricks and the exterior of the second floor of the apartment building is cream colored with dark brown trim in a half-timbered design. The front entrance door leading to the apartments is cream colored and is covered by an awning. The number “6870” is displayed in black on the front of the awning, pictured below:



ATTACHMENT B

Particular Things to be Seized

All records relating to violations of Title 26 United States Code, Section 7206(1) (filing false tax returns) and Section 7206 (2) (aiding or assisting in the filing of false or fraudulent returns), and Title 18 United States Code, Section 287 (false claims). The items to be seized relate to the period January 1, 2020 to the present, maintained by and/or on behalf of Jahnell Easly, Jasmeika Simon, and/or any variations of the business name Unlimited Taxes & More, including:

1. IRS publications, regulations, and/or copies of IRS forms and documents, extracts from the Internal Revenue Code, and any correspondence relating to IRS forms, Internal Revenue Statutes or regulations and tax schedules;
2. Documents or materials related to training in tax law and/or the preparation of tax returns, including but not limited to training manuals, examples, templates, and correspondence in electronic, video, or paper formats;
3. Any internal memos, directives, instructional materials, emails, agreements, and other correspondence between Jahnell Easly, Jasmeika Simon, and other tax preparers and employees of Unlimited Taxes & More;
4. Originals or copies of federal and state income tax returns, income tax forms and tax-return-preparation software, whether blank or completed, and whether filed with the IRS or not;
5. Tax return schedules and forms, tax return worksheets, and other related supporting documents, including but not limited to attachments, questionnaires, work papers, notes, telephone messages, electronic filing documents, correspondence or documents from refund recipients

and/or other tax preparers, and documents relating to deductions and credits claimed on any federal income tax returns;

6. Financial records or information relating to the preparation of client tax returns, including records documenting or purporting to document the receipt of income by a taxpayer or the expenditure of money by a taxpayer, including Forms W-2, employment records, receipts, accounting books and records, bank account records, brokerage account records, checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, images of checks, check stubs, earnings statements, and school or day care records or bills;

7. Financial records or information relating to the receipt and/or status of tax refunds, tax refund loans, or the expenditure of proceeds of such tax refunds or tax refund loans, including but not limited to receipts, bank account records, brokerage account records, U.S. Treasury checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, credit card applications and records, debit card and prepaid credit card applications and records, Refund Anticipation Loan (RAL) applications, RAL checks, and invoices;

8. Personal identification documents, records, or information;

9. Records identifying the taxpayers for whom tax returns have been prepared including client listings, correspondence, telephone books, appointment records, calendars, diaries, notes and other identifying information of the clients;

10. Invoices, receipts, ledgers, schedules, and other records relating to tax consulting or tax preparation fees charged and payments received;

11. Financial records related to Jahnell Easley, Jasmeika Simon, and Unlimited Taxes & More, including, but not limited to, bank account records, bank statements, deposit statements/slips, receipts, cash receipt books, checks, check books, canceled checks, check

registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, invoices and/or bills;

12. Computers or storage media used as a means to commit the violations described above;

13. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smart phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

6870 West Kathleen Court, Apartment 7,
Franklin, Wisconsin 53132

Case No.23-1832M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
26 U.S.C. § 7206(1)	Filing False Tax Returns
26 U.S.C. § 7206 (2)	Aiding or Assisting in the Filing of False or Fraudulent Returns
18 U.S.C. § 287	False Claims

The application is based on these facts:

Please see Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Zachary E. Stegenga Digitally signed by Zachary E. Stegenga
Date: 2023.10.20 11:15:40 -05'00'

Applicant's signature

Zachary E. Stegenga, Special Agent, IRS-CI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

TELEPHONE

(specify reliable electronic means).

Date: 10/23/2023

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Zachary E. Stegenga, being first duly sworn, hereby depose and state as follows:

BACKGROUND AND EXPERIENCE OF AFFIANT

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as, 6870 West Kathleen Court, Apartment 7, Franklin, Wisconsin 53132, hereinafter “Premises,” further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Internal Revenue Service, Criminal Investigation (“IRS-CI”) and have been since October 2008. Through my training and experience I have learned, among other things, financial investigative techniques used to carry out my responsibilities of conducting criminal investigations relating to violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the Bank Secrecy Act (Title 31, United States Code), and other related offenses. I have conducted numerous investigations involving violations of these federal laws. I have been the affiant on numerous search warrants and have participated in the execution of numerous other search warrants.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, and witnesses.

PROBABLE CAUSE

4. As set forth below, there is probable cause to believe that located at the premises identified in paragraph 1 of this affidavit are the fruits, evidence, and instrumentalities of criminal offenses in violation of Title 26, United States Code, Section 7206(1) (filing false tax returns) and Section 7206(2) (aiding or assisting in the filing of false or fraudulent returns), as well as Title 18, United States Code, Section 287 (false claims) (“the Subject Offenses”).

Background

Overview of Return Preparer Fraud Schemes

5. Based on my training, experience, and feedback from other experienced law enforcement officers, I am aware that:

a. Every person who prepares or assists in preparing federal tax returns for compensation must have a Preparer Tax Identification Number (PTIN). PTINs are renewed for every filing season and are used to track the tax preparation activities of paid return preparers.

b. Tax return preparer fraud schemes normally involve multiple false tax returns that appear to have been prepared by the same individual. The tax returns normally share similar tax return characteristics that establish a pattern of fraud.

c. Tax return preparer fraud schemes often involve the electronic filing (e-filing) of false tax returns claiming false earned income amounts in order to qualify taxpayers for maximum refundable credits such as the Earned Income Tax Credit (EITC) and Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals. Often times, the unscrupulous tax return preparers will use false Schedules

C, Profit or Loss From Business, to falsify the earned income amounts. By doing this, the taxpayers receive significantly larger refunds than what they are legitimately owed.

d. Tax return preparers involved in the preparation of false tax returns normally maintain records of their activity, such as copies of tax returns, records of scheme participants including addresses and social security numbers (SSNs), supporting schedules and forms, supporting worksheets, financial records, and bookkeeping records. I know that these records are often stored in both electronic and hardcopy format. Records in electronic format are typically stored on electronic devices, including computers, tablets, and smart phones used to file tax returns electronically. I know that many individuals retain possession of electronic devices and other media for long periods of time, and that individuals involved in the preparation and electronic filing of tax returns maintain the records for long periods of time. These devices and records are typically maintained by tax return preparers in secure locations such as their businesses and residences.

e. Treasury Regulation section 1.6695-2 states that paid tax return preparers are required to meet certain due diligence requirements when preparing returns or claims for refund for clients claiming the EITC, child tax credit, additional child tax credit, credit for other dependents, American opportunity credit, and/or head of household filing status. These due diligence requirements include the retention of certain records for three years from the latest of the following dates: (1) the due date of the tax return, (2) the date the tax return or claim for refund was electronically filed, (3) the date the tax return or claim for refund was presented to the taxpayer for signature if not electronically filed, or (4) if the preparer gives the tax return to another preparer

to complete and sign, the date the preparer submitted it to the signing preparer. The records to be retained for three years include: (1) a copy of the completed Form 8867, Paid Preparer's Due Diligence Checklist, (2) a copy of each completed worksheet for any credits claimed that are specified in the due diligence requirements, (3) a copy of any documents provided by the taxpayer on which the preparer relied to determine the taxpayer's eligibility for the credits and/or head of household filing status and to figure the amounts of the credits claimed, and (4) a record of how, when, and from whom the information used to prepare the Paid Preparer's Due Diligence Checklist and the applicable worksheets was obtained.

Earned Income Tax Credit (EITC)

6. The EITC is a refundable tax credit for working taxpayers who have low to moderate income. This credit will either reduce the tax owed or will generate a refund for the taxpayer. In order to qualify for the EITC, an individual must have earned income under an allowable amount, which changes from year to year. The amount of EITC a taxpayer receives will differ depending on their adjusted gross income (AGI), their filing status, and number of qualifying children. The amount of EITC a taxpayer receives is based on a bell curve. The EITC amount increases with an increase in AGI, up to a certain AGI threshold. As AGI amounts increase above that threshold, the amount of EITC gradually decreases until it reaches the income limitations.

Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals

7. The Families First Coronavirus Response Act (FFCRA), as amended by the COVID-related Tax Relief Act of 2020, provided small and midsize employers refundable tax credits that reimbursed them, dollar-for-dollar, for the cost of providing paid sick and family leave

wages to their employees for leave related to COVID-19, for the time period April 1, 2020, through March 31, 2021. The American Rescue Plan Act of 2021 extended the period for which employers could claim these refundable tax credits to include April 1, 2021, through September 30, 2021. The FFCRA, as amended by the COVID-related Tax Relief Act of 2020, and the American Rescue Plan Act of 2021 extended to self-employed individuals equivalent refundable tax credits against net income. As a result, certain self-employed individuals who were unable to perform their services because they took leave for certain COVID-19 related issues, were eligible to claim these refundable tax credits on Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals, for 2020 and 2021. Forms 7202 were attached to Form 1040, US Individual Income Tax Return, and filed with the IRS.

8. The amount of the Credit for Sick Leave and Family Leave for Certain Self-Employed Individuals was calculated based on the number of days of leave taken for certain COVID-19 related issues, multiplied by the average daily self-employed income of the individual. The amount of this refundable credit increased with an increase in both the number of days of leave taken and the amount of self-employed income up to a certain maximum amount.

Background of the Investigation and Tax Return Patterns

9. I am currently investigating allegations that Jahnell Easley (Easley) and Jasmeika Simon (Simon), tax return preparers for Unlimited Taxes & More (UTM) in Milwaukee, Wisconsin, aided or assisted taxpayers by preparing and filing false federal tax returns with the IRS during the 2022 and 2023 filing seasons. The returns Easley and Simon prepared and filed were for the 2020 through 2022 tax years. These tax returns allegedly reported false Schedule C income and losses, false household employee wages, false sick and family leave credits, and false child and dependent care expenses, among other false items.

10. This investigation began in January 2023 after I received a return preparer fraud scheme referral from the Northern Area Scheme Development Center of the IRS. This referral included an analysis of 2020 and 2021 Forms 1040, US Individual Income Tax Returns, filed with the IRS that list Easly or Simon as the return preparer with their assigned PTINs. The analysis shows that these returns display suspiciously high rates of refunds, Schedule C profits and losses, EITC, credits for child and dependent care, and credits for sick leave and family leave.

11. After receiving the referral from the Northern Area Scheme Development Center of the IRS, I conducted my own analysis of all 2020 through 2022 Form 1040 tax returns filed with the IRS that list Easly or Simon as the return preparer based on their assigned PTINs. As of April 12, 2023, IRS records showed that 702 Form 1040 tax returns listing Easly or Simon as the paid return preparer had been filed with the IRS for the 2020 through 2022 tax years. 99.9% of the tax returns claimed refunds totaling \$11,603,448. The tax returns linked to Easly and Simon as the return preparer list their preparer firm name as UTM. The tax return statistics for the Form 1040 tax returns linked to Easly and Simon were compared to national, state, and local statistics of filed tax returns and are summarized in the tables below:

Form 1040 Tax Returns Claiming Refunds			
Particulars	2020	2021	2022
United States	75.4%	71.7%	70.5%
State of Wisconsin	76.0%	71.4%	69.5%
City of Milwaukee	79.7%	76.3%	73.5%
Jahnell Easly	100.0%	100.0%	100.0%
Jasmeika Simon	100.0%	99.5%	100.0%

Average Refund Amount Claimed on Form 1040 Tax Returns			
Particulars	2020	2021	2022
United States	\$ 2,393.85	\$ 2,519.72	\$ 2,088.07
State of Wisconsin	\$ 2,097.06	\$ 2,101.09	\$ 1,786.56
City of Milwaukee	\$ 2,341.90	\$ 2,691.72	\$ 2,092.26
Jahnell Easley	\$ 12,052.35	\$ 19,653.02	\$ 7,391.67
Jasmeika Simon	\$ 11,555.00	\$ 20,106.99	\$ 9,425.88

Form 1040 Tax Returns Claiming Schedule C Profit or Loss			
Particulars	2020	2021	2022
United States	16.7%	17.8%	17.0%
State of Wisconsin	11.9%	12.8%	12.0%
City of Milwaukee	11.9%	13.7%	13.3%
Jahnell Easley	94.1%	95.0%	56.9%
Jasmeika Simon	100.0%	84.7%	40.0%

Form 1040 Tax Returns Claiming EITC			
Particulars	2020	2021	2022
United States	15.5%	20.2%	15.4%
State of Wisconsin	11.9%	16.0%	10.7%
City of Milwaukee	20.8%	26.5%	20.1%
Jahnell Easley	70.6%	90.6%	78.4%
Jasmeika Simon	77.8%	88.4%	97.5%

Form 1040 Tax Returns Claiming Sick and Family Leave Credits		
Particulars	2020	2021
United States	0.7%	0.7%
State of Wisconsin	0.3%	0.3%
City of Milwaukee	0.5%	1.4%
Jahnell Easley	94.1%	97.5%
Jasmeika Simon	100.0%	94.4%

Form 1040 Tax Returns Claiming Child and Dependent Care Credits	
Particulars	2021
United States	0.3%
State of Wisconsin	0.3%
City of Milwaukee	0.2%
Jahnell Easley	17.6%
Jasmeika Simon	48.6%

12. The statistical comparisons in paragraph 11 show that tax returns prepared and filed by Easley and Simon have suspicious, high rates of tax refunds, Schedule C profits and losses, household employee wages, EITC, credits for child and dependent care, and credits for sick leave and family leave. The tax returns prepared by Easley and Simon also have suspiciously high average refund amounts. Based on my training and experience, these patterns are possible indicators of fraudulent tax return filings.

13. A sampling of Form 1040 tax returns prepared and filed with the IRS by Easley and Simon show significant discrepancies. Based on my training and experience, the following discrepancies are possible indicators of fraudulent tax returns filed to obtain larger tax refunds than legitimately owed to the taxpayers:

a. On February 27, 2022, a 2021 Form 1040 tax return was e-filed with the IRS in the name of a taxpayer with initials M.J. This tax return lists Easly as the paid tax preparer with her assigned PTIN. The refund amount on this tax return is \$30,063. There is a Form 2441, Child and Dependent Care Expenses, attached to this tax return that lists Easly as the care provider for M.J.'s four qualifying dependents and shows that Easly was paid \$15,680 for her services. This resulted in a refundable tax credit of \$7,840. In contrast, Easly did not report any income as a child care provider on her own 2021 Form 1040 tax return. This same tax return reported a Schedule C, Profit or Loss From Business, listing M.J. as the owner of an "Apparel Mfg" business. The Schedule C claimed a loss of \$6,390 based on a single line entry for supplies expenses of \$6,390. There was no other self-employment income reported on the tax return. In contrast, the Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals, reported \$17,550 of net earnings from self-employment for calculating the refundable credit.

b. On April 18, 2022, a 2021 Form 1040 tax return was e-filed with the IRS in the name of a taxpayer with initials C.G. This tax return lists Simon as the paid tax preparer with her assigned PTIN. The refund amount on this tax return is \$25,280. This tax return reported a Schedule C, Profit or Loss From Business, listing C.G. as the owner of a "Beauty Salons" business. The Schedule C claimed a profit of \$18,600. There was no other self-employment income reported on the tax return. In contrast, the Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals, reported \$41,677 of net earnings from self-employment for calculating the refundable credit.

Jahnell Easley's Form 1040 Tax Returns

14. Easley self-prepared and filed personal 2021 and 2022 Form 1040 tax returns with the IRS that display significant discrepancies. Based on my training and experience, the following discrepancies are possible indicators of fraudulent tax returns filed by Easley to falsely increase her tax refunds:

a. On January 30, 2022, Easley e-filed a self-prepared, personal 2021 Form 1040 tax return with the IRS. Easley reported a tax refund of \$4,370 on this return. This return reported a Schedule C self-employment loss of \$5,020 for a credit repair business named Nells Business Services. There was no other self-employment income reported on the tax return. In contrast, the attached Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals, reported \$29,500 of net earnings from self-employment for calculating a \$2,260 refundable credit for sick leave.

b. On April 26, 2023, Easley e-filed a 2021 Form 1040X, Amended US Individual Tax Return, with the IRS and listed her home address as 6870 W Kathleen Ct, Apt 7, Franklin, WI 53132. Easley is listed as the paid preparer on the return. Easley reported a tax refund of \$16,150 on the return. This return amended multiple items, including the Schedule C and Form 7202. The Schedule C self-employment loss of \$5,020 for Nells Business Services was amended to show a profit of \$2,430. The Form 7202 was amended to include the addition of a family leave credit and the net earnings from self-employment was increased from \$29,500 to \$56,744, which is conflicting with the Schedule C self-employment profit of \$2,430. This resulted in a significant increase to the Form 7202 credits and the tax refund.

c. On April 4, 2023, Easly e-filed a self-prepared, personal 2022 Form 1040 tax return with the IRS and listed her home address of 6870 W Kathleen Ct, Apt 7, Franklin, WI 53132. Easly reported a tax refund of \$9,250 on the return. The only income reported on the return was a Schedule C self-employment profit of \$20,213 from a tax preparation business named J&J Taxes and More Credit Repair. The Schedule C reported sales of \$28,567, \$6,000 of rent, and \$2,354 of supplies. In contrast, IRS records show that Easly was issued a 2022 Form 1099-NEC, Nonemployee Compensation, from Unlimited Taxes and More Inc for \$229,117 of taxable nonemployee compensation and a Form 1099-NEC from Unlimited Taxes and More Franchising for \$14,352 of taxable nonemployee compensation. These Forms 1099-NEC or the taxable amounts were not reported anywhere on Easly's 2022 Form 1040. Additionally, the return reported a \$12,574 refundable fuel tax credit, claimed on Form 4136, Credit for Federal Tax Paid on Fuels. Easly reported the nontaxable use of 58,762 gallons of gasoline for off-highway business use and 9,952 gallons of gasoline for use on a farm for farming purposes on the Form 4136. Based on the U.S. Energy Information Administration (EIA) website, www.eia.gov, the average price of a gallon of gasoline, which includes all grades of gasoline, was \$4.059 in 2022. Using this average, the 68,714 gallons of gasoline that Easly claimed to have purchased and used would have cost \$278,910. In contrast, she only reported \$28,567 of sales for the year. Also, there is no Schedule F, Profit or Loss From Farming, claimed on the return or any farming related activity reported elsewhere on the return to support Easly's claim that she used 13,591 gallons of gasoline for use on a farm for farming purposes. Based

on this, I believe Easley falsely inflated the number of gallons of gasoline she claimed on this Form 4136 to increase her tax refund.

Jasmeika Simon's Form 1040 Tax Returns

15. Simon self-prepared and filed personal 2021 and 2022 Form 1040 tax returns with the IRS that display significant discrepancies. Based on my training and experience, the following discrepancies are possible indicators of fraudulent tax returns filed by Simon to falsely increase her tax refunds:

a. On January 21, 2022, Simon e-filed a personal 2021 Form 1040 tax return with the IRS. Simon is listed as the paid preparer on the return. Simon reported a tax refund of \$18,198 on the return. The only income reported on the return was \$10,500 of household help wages. There was no self-employment income reported. In contrast, Simon attached a Form 7202, Credits for Sick Leave and Family Leave for Certain Self-Employed Individuals, reporting \$20,500 of net earnings from self-employment for calculating refundable credits for sick and family leave of \$4,230. Additionally, Simon reported \$7,980 of child and dependent care expenses for a refundable credit of \$3,990. The child and dependent care expenses Simon reported represent 76% of her total income reported on this tax return. This would have left Simon and her dependent with only \$2,520 for basic living expenses. Based on this discrepancy and my analysis of suspicious child and dependent care credits Simon reported on her clients' tax returns, I believe Simon's child and dependent care credit claim was falsely inflated to increase Simon's tax refund.

b. On April 17, 2023, Simon e-filed a self-prepared, personal 2022 Form 1040 tax return with the IRS. Simon reported a tax refund of \$10,249 on the return. The

only income reported on this return was a Schedule C self-employment profit of \$21,213 from a general freight business named High Speed Logistics MKE LLC. The Schedule C reported sales of \$29,567, \$6,000 of rent, and \$2,354 of supplies. In contrast, IRS records show that Simon was issued a 2022 Form 1099-NEC, Nonemployee Compensation, from Unlimited Taxes and More Inc for \$208,950 of taxable nonemployee compensation and a Form 1099-NEC from Unlimited Taxes and More Franchising for \$35,400 of taxable nonemployee compensation. These Forms 1099-NEC were not reported anywhere on Simon's 2022 Form 1040. Additionally, this return reported a \$13,789 refundable fuel tax credit, claimed on Form 4136, Credit for Federal Tax Paid on Fuels. Simon reported the nontaxable use of 61,762 gallons of gasoline for off-highway business use and 13,591 gallons of gasoline for use on a farm for farming purposes on the Form 4136. As discussed in paragraph 14(c) above, based on the average price of a gallon of gasoline in 2022 per EIA, the 75,353 gallons of gasoline that Simon claimed to have purchased and used would have cost \$305,857. In contrast, she only reported \$29,567 of sales. Also, there is no Schedule F, Profit or Loss From Farming, claimed on the return or any farming related activity reported elsewhere on the return to support Simon's claim that she used 13,591 gallons of gasoline for use on a farm for farming purposes. Based on this, I believe Simon falsely inflated the number of gallons of gasoline she claimed on this Form 4136 to increase her tax refund.

Undercover Operation

16. On March 7, 2023, an Internal Revenue Service, Criminal Investigation Undercover Agent (UCA) went to UTM located at 8247 W Brown Deer Road, Milwaukee,

Wisconsin 53223, in an undercover capacity, to have a federal income tax return prepared by Easly. This meeting was scheduled between Easly and the UCA; however, when the UCA arrived at UTM, the doors were locked and the lights were off. The UCA subsequently called Easly at phone number 262-888-2951 and spoke to her. Easly told the UCA that she forgot about the meeting. During the phone call, they arranged for Easly to prepare the UCA's tax return remotely. Easly told the UCA she would text and email a virtual link to the UCA to upload personal and tax information for Easly to use to prepare the tax return.

17. On March 7, 2023, Easly text messaged the UCA the following link: <https://www.cognitoforms.com/UTM6/TaxClientIntakeForm>. This is the same link that was displayed in the "Intro" section of Subject Account 1 when I conducted surveillance on January 13, 2023. Easly emailed the link to the UCA from email address, jahnelleasly01@gmail.com and carbon copied jeasly@unlimitedtaxestx.com. The UCA subsequently navigated to the Tax Client Intake Form via the link and was taken to the following screen:

12:48 LTE

Done cognitoforms.com AA

Dream Team
INVESTMENT GROUP
UNLIMITED
TAXES & MORE, INC.
POWERED BY
"THE AFFORDABLE PROFESSIONAL ALTERNATIVE"

Tax Client Intake Form

Taxpayer Information

Tax Preparer : Jahnell Easley

Email: Jeasly@Unlimitedtaxestx.com

Phone: 262-888-2951

Location: 8247 W Browndeer Rd Milwaukee, WI 53223

Did you file with us last Filing Tax Year *

18. After navigating to the Tax Client Intake Form, the UCA entered the following information and submitted it:

- a. The UCA's name, phone number, email address, social security number, date of birth, and occupation.
- b. The UCA uploaded a photocopy of the UCA's driver's license and social security card.
- c. The names, dates of birth, social security numbers, and relationships for two dependent children.
- d. The UCA uploaded a photocopy of the UCA's 2022 Form W-2, Wage and Tax Statement. This Form W-2 lists Box 1 wages of \$1,144 and Box 2 federal income tax withheld of \$0.

e. The UCA signed the following: (1) I certify I would like to have my tax return prepared in accordance with the information I have provided, (2) Consent to Use of Tax Return Information, and (3) Consent to Disclosure of Tax Return Information.

19. If a 2022 Form 1040 was prepared accurately based on the information entered into the Tax Client Intake Form by the UCA, it would have produced a federal tax refund of \$450.

20. On March 8, 2023, at approximately 2:41 PM, Easly text messaged the UCA, asking for proof of the UCA's kids. On March 9, 2023, at approximately 12:15 AM, the UCA responded to Easly by texting a photocopy of the social security cards for both of the UCA's dependents.

21. On March 9, 2023, at approximately 1:00 PM, Easly called the UCA. This phone call was consensually recorded by the UCA. I have personally listened to the recording of this phone call. The following exchange occurred during the phone call:

EASLY: So I can give you two alternatives.

UCA: Mm-hmm.

EASLY: We can use the- we can use the tax form, the-the W2 that you have, which is not ultimately giving you nothing for the children that you're filing.

UCA: Mm-hmm.

EASLY: Or I can add like a self-employment on there like you did hair or anything of that nature on there, and you pretty much can go about it that route and have employment on there.

UCA: Okay. Well, [coughs] oh, I'm sorry. I got real sick last night and this morning, but um, I-- whichever way, 'cause they told me you were good at whatever you did, so I'm just-- I'm fine with however you do it. Yes--

EASLY: Okay. So I'm gonna let you know what--

UCA: Mm-hmm.

EASLY: I'm gonna put you as like a hairstylist or something. Um, I'm gonna let you know the numbers. I just wanted to get your permission to do so--

UCA: Uh-huh.

EASLY: -before I do it because some people (unintelligible) they stuff done regularly. Whatever they get back, they get back. But I just wanna always give you that option, you know.

22. On March 10, 2023, Easly emailed the UCA a copy of the UCA's 2022 Form 1040 and supporting files from email address jeasly@unlimitedtaxestx.com. This tax return was compared to the 2022 Form 1040 filed with the IRS in the UCA's identity and the returns match. This tax return reported multiple false income items that were not provided to Easly by the UCA. This tax return reported \$12,153 of false household employee wages on Form 1040 line 1b and \$7,593 of false profit from a Schedule C, Profit or Loss From Business, claiming the UCA operated a business as a hair braider. By adding the false household employee wages and business income, Easly fraudulently increased the UCA's tax refund by \$7,268 to \$7,718.

Internet Protocol (IP) Address Records

23. IRS records show that 13 of the Form 1040 tax returns listing Easly as the paid preparer between January 25, 2023 and March 7, 2023 were filed from IP address 65.31.106.194 or 70.92.131.78. Both of these IP addresses belong to Charter Communications. Charter Communications records were obtained and they show that IP address 65.31.106.194 and 70.92.131.78 were assigned to Easly's subscriber account during the time period when each of the 13 tax returns was filed with the IRS. The service and billing address for Easly's subscriber account is 6870 W Kathleen Ct, Apt 7, Franklin, WI 53132 ("Premises"). Thus, there is probable cause to believe that located at the Premises will be records relating to the filing of false tax returns and electronic devices which contain evidence relating to the e-filing of false tax returns.

24. IRS records show that 40 of the Form 1040 tax returns prepared by Easly and Simon between October 17, 2022 and April 11, 2023 were filed from IP address 70.92.0.87, 70.92.133.110, 70.92.144.157, or 70.92.3.126. These IP addresses belong to Charter Communications. Charter Communications records were obtained and they show that these IP addresses were assigned to Simon's subscriber account during the time when each of the 40 tax returns was filed with the IRS. The service and billing address for Simon's subscriber account is 2806 W Howard Ave, Apt 2, Milwaukee, WI 53221 (Simon's residence).

Surveillance

25. On September 8, 2023, I conducted surveillance at 6870 West Kathleen Court, Franklin, Wisconsin (Premises). At approximately 7:30AM, I observed a black Volvo XC90 vehicle with Wisconsin license plate number ARL8132 parked in a parking lot adjacent to 6870 West Kathleen Court. At approximately 7:40AM, I observed two individuals, one of which was Easly, walk to the Volvo XC90 from the rear of the building at 6870 West Kathleen Court. Easly

entered the driver door of the vehicle and the unknown individual entered the passenger side door. Then, Easley drove away from the area.

Additional Indicia of Residency

26. United States Postal Service records for the period June 20, 2023 to July 19, 2023 show numerous mailings were sent to Easley at 6870 West Kathleen Court, Apartment 7, Franklin, Wisconsin 53132. This includes mailings from the IRS, Wisconsin Department of Transportation (WI DOT), and Spectrum (Charter Communications).

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, such as the fact that returns were filed electronically, I am aware that computer equipment was used to generate, store, and print documents used in the scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

30. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how

and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to e-file fraudulent tax returns, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit

a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. Based on the foregoing, there is probable cause to believe that items described in Attachment B of this affidavit are evidence of the crimes described in this affidavit and are currently located at the premises, more particularly described in Attachment A. I respectfully request that the Court issue the proposed search warrant.

ATTACHMENT A

Property to Be Searched

The residence of Jahnell Easley, 6870 West Kathleen Court, Apartment 7, Franklin, Wisconsin, 53132. Apartment 7 is on the first floor of the north entrance to a two story apartment building. The exterior of the first floor of the apartment building has brown bricks and the exterior of the second floor of the apartment building is cream colored with dark brown trim in a half-timbered design. The front entrance door leading to the apartments is cream colored and is covered by an awning. The number “6870” is displayed in black on the front of the awning, pictured below:



ATTACHMENT B

Particular Things to be Seized

All records relating to violations of Title 26 United States Code, Section 7206(1) (filing false tax returns) and Section 7206 (2) (aiding or assisting in the filing of false or fraudulent returns), and Title 18 United States Code, Section 287 (false claims). The items to be seized relate to the period January 1, 2020 to the present, maintained by and/or on behalf of Jahnell Easley, Jasmeika Simon, and/or any variations of the business name Unlimited Taxes & More, including:

1. IRS publications, regulations, and/or copies of IRS forms and documents, extracts from the Internal Revenue Code, and any correspondence relating to IRS forms, Internal Revenue Statutes or regulations and tax schedules;
2. Documents or materials related to training in tax law and/or the preparation of tax returns, including but not limited to training manuals, examples, templates, and correspondence in electronic, video, or paper formats;
3. Any internal memos, directives, instructional materials, emails, agreements, and other correspondence between Jahnell Easley, Jasmeika Simon, and other tax preparers and employees of Unlimited Taxes & More;
4. Originals or copies of federal and state income tax returns, income tax forms and tax-return-preparation software, whether blank or completed, and whether filed with the IRS or not;
5. Tax return schedules and forms, tax return worksheets, and other related supporting documents, including but not limited to attachments, questionnaires, work papers, notes, telephone messages, electronic filing documents, correspondence or documents from refund recipients

and/or other tax preparers, and documents relating to deductions and credits claimed on any federal income tax returns;

6. Financial records or information relating to the preparation of client tax returns, including records documenting or purporting to document the receipt of income by a taxpayer or the expenditure of money by a taxpayer, including Forms W-2, employment records, receipts, accounting books and records, bank account records, brokerage account records, checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, images of checks, check stubs, earnings statements, and school or day care records or bills;

7. Financial records or information relating to the receipt and/or status of tax refunds, tax refund loans, or the expenditure of proceeds of such tax refunds or tax refund loans, including but not limited to receipts, bank account records, brokerage account records, U.S. Treasury checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, credit card applications and records, debit card and prepaid credit card applications and records, Refund Anticipation Loan (RAL) applications, RAL checks, and invoices;

8. Personal identification documents, records, or information;

9. Records identifying the taxpayers for whom tax returns have been prepared including client listings, correspondence, telephone books, appointment records, calendars, diaries, notes and other identifying information of the clients;

10. Invoices, receipts, ledgers, schedules, and other records relating to tax consulting or tax preparation fees charged and payments received;

11. Financial records related to Jahnell Easley, Jasmeika Simon, and Unlimited Taxes & More, including, but not limited to, bank account records, bank statements, deposit statements/slips, receipts, cash receipt books, checks, check books, canceled checks, check

registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, invoices and/or bills;

12. Computers or storage media used as a means to commit the violations described above;

13. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smart phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.